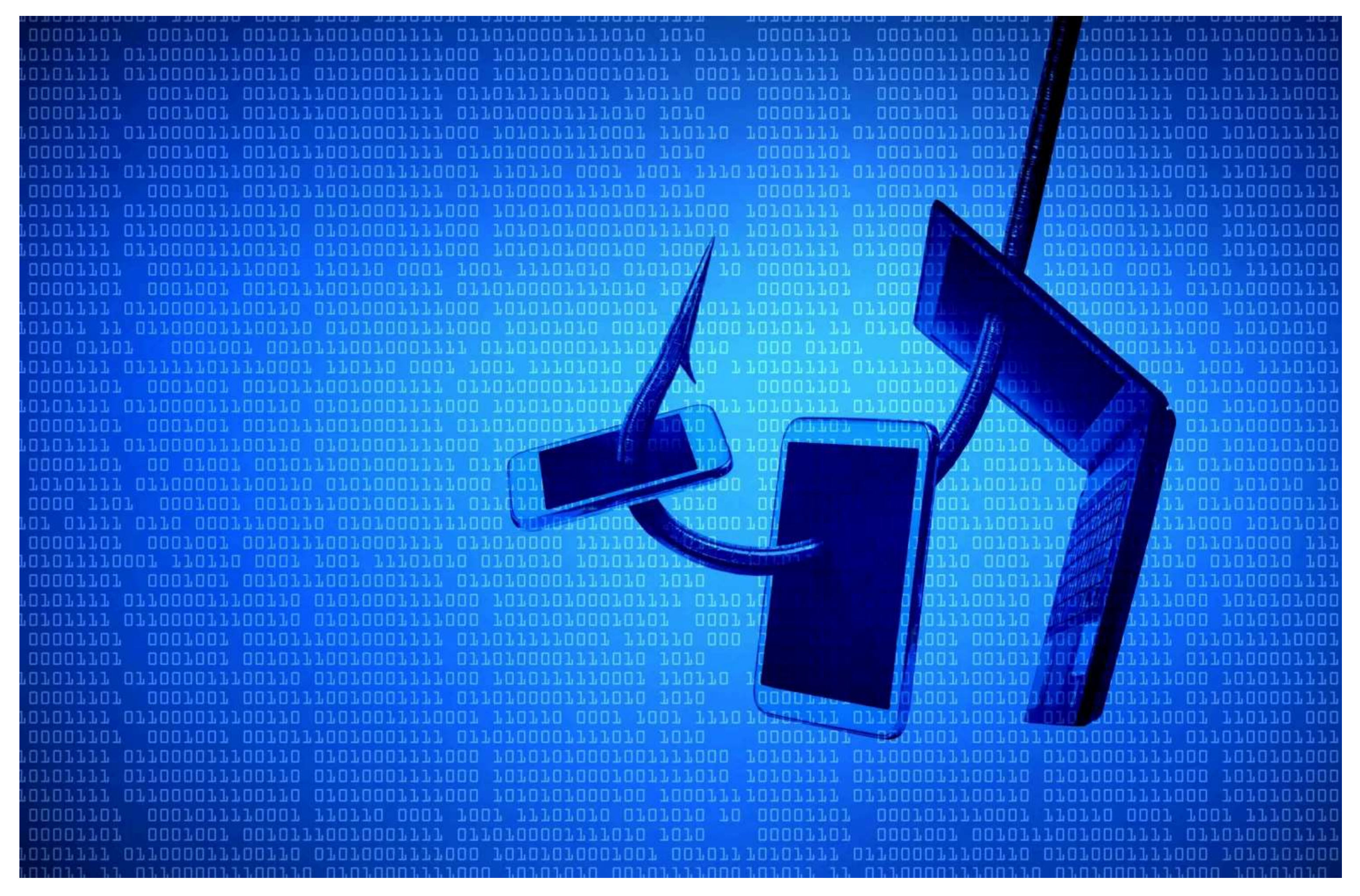
تكنولوجيا

كيف يعيد الذكاء الاصطناعي والحوسبة الكمومية تشكيل الأمن السيبراني في 2025؟

«الشرق الأوسط» تحاور «بالو ألتو نتوركس» حول مستقبل الأمن السيبراني الذكي



تتضمن الاتجاهات الرئيسة لعام 2025 الاستعداد الكمومي وممارسات الأمن السيبراني الخضراء والامتثال (شاترستوك)

لندن: نسيم رمضان

نُشر: 13:43-19 ديسمبر 2024 م ـ 17 جمادى الآخرة 1446 هـ

بينما تواجه المنظمات والشركات تهديدات سيبرانية متطورة، أصبحت تقنيات مثل الذكاء الاصطناعي والحوسبة الكمومية والمنصات الأمنية الموحدة حاسمة في المشهد الحالي. لا تقتصر هذه الابتكارات على معالجة التهديدات الفورية فحسب، بل تساعد أيضاً في الاستعداد لتحديات المستقبل.

تحويل مراكز العمليات الأمنية

يلعب الذكاء الاصطناعي دوراً محورياً في الأمن السيبراني، خاصة داخل مراكز العمليات الأمنية (SOCs). مع تزايد تعقيد الهجمات المدعومة بالذكاء الاصطناعي، تتوجه المنظمات نحو منصات بيانات موحدة لتعزيز الرؤية والاستجابة. يوضح حيدر باشا، الرئيس التنفيذي لأمن المعلومات لدى شركة «بالو ألتو نتوركس» لمنطقة أوروبا والشرق الأوسط وأفريقيا وأميركا اللاتينية، خلال حديث خاص لـ«الشرق الأوسط» أن المنصات الموحدة لمراكز العمليات الأمنية تتيح دمج الرؤية والتحليلات والاستجابة، مما يعزز القدرة على اكتشاف التهديدات بشكل أسرع وأتمتة أولوياتها. وتعزز منصات مثل «Cortex XSIAM» لدى «بالو ألتو نتوركس» الكفاءة من خلال أتمتة المهام المتكررة، مما يسمح للمحللين بالتركيز على تفسير نتائج الذكاء الاصطناعي وصيد التهديدات، مما يعزز المرونة بحسب وصفه.



حيدر باشا الرئيس التنفيذي لأمن المعلومات لدى شركة «بالو ألتو نتوركس» لمنطقة أوروبا والشرق الأوسط وأفريقيا وأميركا اللاتينية (Palo Alto)

تأثير الذكاء الاصطناعي

مع تحول الذكاء الاصطناعي إلى مساعد في العمليات الأمنية، تتغير طبيعة الأدوار البشرية. توفر الأدوات المدعومة بالذكاء الاصطناعي إمكانيات أتمتة للكشف عن التهديدات، مما يتطلب إعادة تعريف الوظائف التقليدية. يقول باشا إن المحللين سيتحولون إلى التركيز على مهارات أعلى، مثل تفسير مخرجات الذكاء الاصطناعي وصيد التهديدات. ويوضح أن المنظمات تحتاج إلى الاستثمار في تدريب فرقها على أخلاقيات الذكاء الاصطناعي واستجابة الحوادث الاستراتيجية لضمان التعاون السلس بين البشر والذكاء الاصطناعي.

الأمن المقاوم للكمّ

لم تعد الحوسبة الكموميّة مجرد احتمال بعيد. وبينما لا تزال الهجمات الكمومية الفعلية على أساليب التشفير واسعة الانتشار غير ممكنة، ويُتوقع أن تصبح واقعاً خلال العقد المقبل. يعزز هذا الحاجة إلى خريطة طريق للأمن المقاوم للكم يشرحها حيدر باشا بالعناصر التالية:

- **تقييم المخاطر**: يجب على المؤسسات تحديد التطبيقات والتقنيات التي تحتاج إلى التشفير المقاوم للكم.

- **الهجرة التدريجية**: الانتقال إلى خوارزميات مقاومة للكم، مع مراعاة التأثيرات على الأجهزة وتأخيرات الأداء.

- **التعاون مع القادة**: التنسيق مع الأولويات المؤسسية لتعظيم إمكانيات الكم في تقليل استهلاك الطاقة وتحسين أحمال الذكاء الاصطناعي.

ويعُدّ باشا خلال حديثه إلى «الشرق الأوسط» أن «الاستراتيجيات الفورية تشمل تطبيق التشفير الهجين والاستعداد لمعايير ما بعد الكم». يضمن هذا النهج الثنائي دفاعات فعالة ضد التهديدات الناشئة.



تعمل أدوات الذكاء الاصطناعي على أتمتة اكتشاف التهديدات وإعادة تعريف الأدوار البشرية للتركيز على التكتيكات المتقدمة (أدوبي)

كسر الصوامع الأمنية

أحد المحاور الرئيسة لتوقعات «بالو ألتو نتوركس» (Palo Alto Networks) للمستقبل هو الاتجاه نحو المنصات الموحدة التي تدمج أدوات الأمن السيبراني المختلفة. تسهّل هذه المنصات العمليات وتعزز الكفاءة، خاصة للمؤسسات الصغيرة ذات الموارد المحدودة. ويشرح باشا أنه يمكن للشركات الصغيرة تسوية ساحة اللعب من خلال خدمات مُدارة تعتمد على الذكاء الاصطناعي. ويوضح أن الشراكات مع مقدمي الحلول تتيح الوصول إلى التحليلات السلوكية والدفاعات المؤتمتة دون الحاجة إلى بيانات ضخمة. كما أن المنصات الموحدة أيضاً تدعم بنى الثقة الصفرية، وهو أمر بالغ الأهمية مع توسع الهجمات في نماذج العمل الهجين.

دور الأمن السيبراني في الاستدامة

مع تبني الممارسات البيئية، يجب أن تتماشى فرق الأمن السيبراني مع الأولويات البيئية. تقلل الابتكارات مثل التعلم الفيدرالي (وهو نهج مبتكر في مجال التعلم الآلي يهدف إلى تدريب نماذج الذكاء الاصطناعي على كميات هائلة من البيانات دون الحاجة إلى جمعها في مكان مركزي واحد) ونماذج

الذكاء الاصطناعي الخفيفة من استهلاك الطاقة. ويشدد حيدر باشا على أن الاستدامة تبدأ بتحسين الخوارزميات واستخدام مراكز بيانات صديقة للبيئة. علاوة على ذلك يقول: «تمتلك أطر الكمّ إمكانات لتحسين كفاءة الطاقة في أحمال الذكاء الاصطناعي».

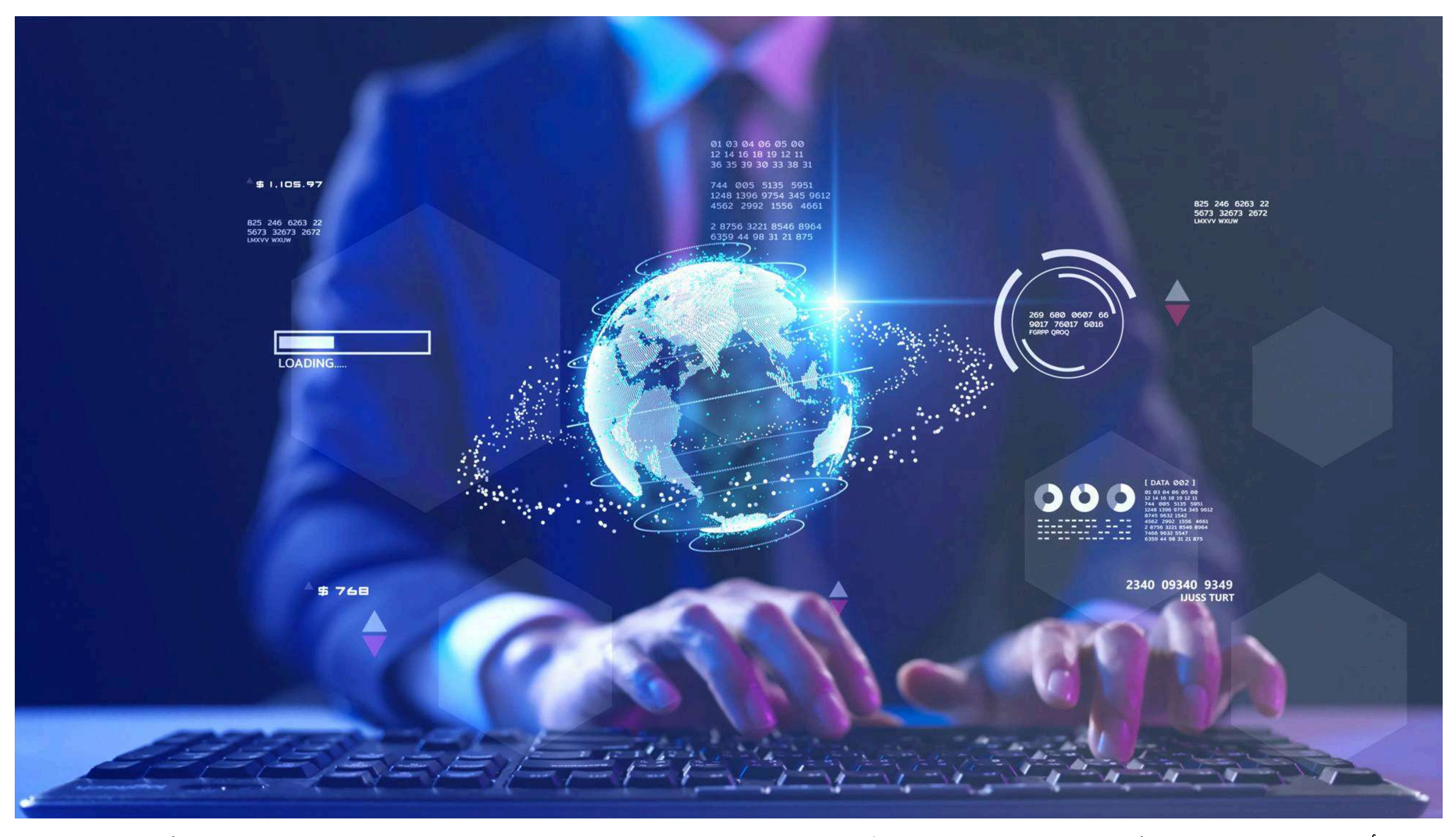
الذكاء الاصطناعي والخصوصية

مع تحول أنظمة الذكاء الاصطناعي إلى عنصر أساسي في الأمن السيبراني، يصبح ضمان الشفافية والاستخدام الأخلاقي أمراً بالغ الأهمية. يؤكد باشا على أهمية الذكاء الاصطناعي القابل للتفسير والتقنيات التي تحافظ على الخصوصية. ويقول: «يجب على المنظمات إعطاء الأولوية للتفسير، مما يُظهر كيفية اتخاذ قرارات الذكاء الاصطناعي مع دمج تقنيات الحفاظ على الخصوصية مثل الخصوصية التفاضلية».

تعزز هذه الخطوات ثقة العملاء وتتوافق مع أطر تنظيمية مثل النظام الأوروبي العام لحماية البيانات (GDPR).

في المستقبل، سيدفع التقاطع بين الذكاء الاصطناعي والأمن السيبراني وتقنيات الاتصال الناشئة مثل الجيل السادس للاتصالات الخلوية (6G) لتغييرات جذرية. بحلول عام 2030، يُتوقع أن يدير الذكاء الاصطناعي الكشف عن التهديدات والاستجابة بشكل مستقل. ويرى باشا أن هذا التقاطع سيمكّن أمان «إنترنت الأشياء» على نطاق غير مسبوق، مما يضمن حماية المليارات من الأجهزة المتصلة دون تدخل بشري.

تسهل هذه التطورات أيضاً تقسيم الشبكات، مما يتيح للشركات تخصيص حلول للأمن السيبراني حسب حالات الاستخدام بحسب رأيه.



"بالو ألتو نتوركس": يتطلب الأمن السيبراني مستقبلا حلولاً تعاونية قابلة للتكيّف والموازنة بين التهديدات الفورية والاستعداد طويل الأجل (شاترستوك)

مشهد الأمن السيبراني في عام 2025

حددت «بالو ألتو نتوركس» (Palo Alto Networks) خمسة اتجاهات رئيسة من المتوقع أن تشكل الأمن السيبراني بحلول عام 2025، وهي:

- **الجاهزية الكمومية:** ستتكثف الجهود لنشر خوارزميات مقاومة للكمّ، خاصة في الخدمات المالية والبنية التحتية الوطنية.

- **مقاييس الذكاء الاصطناعي للأمن السيبراني**: ستتبنى المنظمات مؤشرات أداء رئيسة لقياس فاعلية الأمن المدعوم بالذكاء الاصطناعي.

- **إعادة تعريف الأدوار الوظيفية**: سيؤدي الذكاء الاصطناعي المساعد إلى تغيير وصف الوظائف الأمنية.

-**الممارسات السيبرانية المستدامة**: ستؤدي المبادرات الخضراء إلى تعزيز وتحسين نماذج الذكاء الاصطناعي.

- **الامتثال التنظيمي**: ستصبح الأدلة الفورية على تأثير الأمن السيبراني أمراً ضرورياً في عمليات التدقيق.

بناء دفاعات سيبرانية مرنة

يشهد مشهد الأمن السيبراني تحولاً جذرياً مدفوعاً بتقدم الذكاء الاصطناعي والحوسبة الكمومية والمنصات الموحدة. مع تقارب هذه التقنيات، فإنها تَعد بتحسين الكفاءة والاستدامة في العمليات الأمنية.

يلخص حيدر باشا هذا التصور قائلاً: «نركز على تقديم حلول تكيفية وشفافة ومواكبة للمستقبل. من خلال مواءمة التكنولوجيا مع الأولويات المؤسسية، نضمن بقاء الأعمال آمنة ومبتكرة في مواجهة المشهد المتغير للتهديدات».

بالنسبة للمؤسسات من جميع الأحجام، يكمن التحدي في موازنة التهديدات الفورية مع الاستعداد طويل الأمد. سواء من خلال مراكز العمليات الأمنية المدعومة بالذكاء الاصطناعي، استراتيجيات مقاومة الكم، أو الممارسات المستدامة، يتطلب الطريق إلى الأمام نهجاً تعاونياً واستباقياً. فمع اقتراب عام 2025، ستصبح هذه الأدوات لا غنى عنها للتعامل مع هذه التعقيدات.

